Opening Remarks of FTC Chairwoman Edith Ramirez
Fall Technology Series: Ransomware
Washington, D.C.
September 7, 2016

Good afternoon and welcome to the Federal Trade Commission's workshop on ransomware. This is the first in a series of events that we are hosting this fall to examine the consumer protection implications of new and evolving technologies.

From the earliest days of the Internet, criminals have used an array of tactics to trick consumers into downloading malware, spyware, and other unwanted software onto their computers and devices.[1] This software makes our computers more vulnerable to viruses, allows scammers to monitor consumers' online activity, and provides a pathway for them to steal personal information, which they can then use to perpetrate fraud.

In recent years, criminals have found a new business model for this kind of malicious activity in the form of ransomware. This type of malware infiltrates a computer system and uses tools like encryption to hold valuable data "hostage" in exchange for a ransom. By charging victims for the return of their data, criminals have created a new market for personal information, making ransomware even more profitable than other scams.

challenges ransomware poses. The perpetrators took out the hospital's entire network for more than a week, leaving staff without access to email and critical patient data. The malware crippled the hospital's emergency room systems and other computer systems necessary for patient care, and forced hospital staff to log medical records with pen and paper. Ultimately, the hospital paid a ransom of 40 b

unlikely to go away any time soon. According to data from Cyence, Inc., typical ransomware payments range from $500 to $1,000, but some criminals have demanded as much as $30,000.[6]

The perpetrators of ransomware attacks are also using a wide range of tactics to lure their targets into downloading malicious software. They used to rely on spam e-mail to deliver ransomware. But as spam filters have grown better at blocking these messages, attackers have turned to spear phishing targeting specific individuals or organizations.[7] According to

consumers. For example, ransomware attackers may be able to steal extremely sensitive consumer information, such as medical information, financial account numbers, and the contents of private communications, some of which may be sold on the dark web. And by shutting down companies' ability to operate, attackers can deny essential and even life-saving services to consumers, such as access to medical records in an emergency.

In light of the significant risk of harm that ransomware poses, as well as the increase in the number and sophistication of attacks, we are eager to expand our understanding of this growing threat.

II. Role of the Federal Trade Commission

As an agency that has long addressed the harm caused by malware, including the

One component of reasonable security is that companies have procedures in place to address vulnerabilities as they arise, including malicious software. A company's unreasonable failure to patch vulnerabilities known to be exploited by ransomware might violate the FTC Act. For example, in a recent case against device manufacturer, ASUS, we alleged that the company's pervasive security bugs left the company's routers vulnerable to malware, and that attackers exploited these vulnerabilities to reconfigure consumers' security settings and take control of consumers' web activity. We also alleged that the company did not address these security vulnerabilities in a timely manner and did not notify consumers about the risks posed by their vulnerable routers.

In another case against Wyndham Worldwide, we alleged that hackers infiltrated the network of a Wyndham franchisee, navigated to the company's network and the networks of other franchisees, and placed memory-scraping malware on the franchisees' servers. We alleged that these hackers exploited Wyndham's lax security to steal sensitive consumer data from dozens of Wyndham franchisees.

As these cases illustrate, businesses play a critical role in ensuring that they adequately protect consumers' information, particularly as security threats like ransomware escalate.

III. Overview of Ransomware Workshop

As we continue to learn more about the impact and scope of ransomware attacks, we find ourselves facing a number of questions. For example, are there steps consumers and businesses should be taking to reduce the risk of ransomware or decrease its impact? What can be learned from criminal law enforcement's efforts to combat these attacks? If you fall prey to ransomware, should you pay the ransom? These are just a few of the questions that we will attempt to answer during today's workshop. My hope is that this discussion will provide valuable insight into the